UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,413	07/05/2005	Shunji Harada	2005_1051A	7700

513 7590 04/30/2007
WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
04/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/541,413	**Applicant(s)** HARADA ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _05 July 2005_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-23_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-23_ is/are rejected.

7)□ Claim(s) _1, 9, 15, 17, 21 and 22_ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _05 July 2005_ is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _7/5/2005_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 7/5/2005 but is a 371 case of PCT/JP04/01934 application filed 2/9/2004 and has a foreign priority application filed on 2/21/2003.

Claim Objection

2. Claims 1, 15, 21 and 22 are objected because the claim language "a receiving unit operable to receive the instruction from the recording medium" is suggested to be corrected with more proper claim language because a regular recording medium as described in the instant specification (SPEC: Page 2 Line 18 – 19: a removable recording medium is inserted in a cartridge containing a volatile storage area and a nonvolatile storage area) cannot determine and provide the instruction to a receiving unit whether the permission should be granted or not based on the stored license usage information in the lack of processing units.

Examiner respectfully suggests to amend the claim language from "a recording medium" to "a memory card (or IC card)" that contains not only storage units but also security processing units that can issue instruction to a receiving unit according to the instant specification (SPEC: Figure 2 / Element 220 / 231 / 214 and Page 2 Line 3 – 4: e.g. a MEMORY CARD).

3. Claim 20 is objected because the claim language "The computer problem" should be "The computer program". Appropriate correction is required.

4. Claims 9 and 17 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of their base / independent claims 5 and claim 15 respectively because the claim limitations of claim 9 and 17 are self-conflicting (i.e. self-contradicting) to their base claims with the following reasons:

- Claim 5 and 15 recite: "a tamper-resistant module operable to judge, based on the license information, whether an operation, ···, is permitted, and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted"; and

- Claim 9 and 17 recite: "the tamper-resistant module, when installation is judged to be permitted, extracts the signature data from the license information, and outputs the extracted signature data instead of the instruction (i.e. instead of the instruction showing that the operation is permitted)".

- Examiner notes such a conflict claim limitation is respectfully to be corrected because the base claim indicates when installation is judged to be permitted, outputting an instruction showing that the operation is permitted while its dependent claim recites **not** outputting an instruction showing that the operation is permitted. According to MPEP § 608.01(n)(II) & (III), the test as to whether a claim is a proper dependent claim is that it shall include every limitation of the claim from which it depends or in other words that it shall not conceivably be infringed by anything which would not also infringe the basic claim. See MPEP § 608.01(n)(II) & (III).

- Applicant is required to cancel the claims, or amend the claims to place the claims in proper dependent form, or rewrite the claims in independent form.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 19 and 22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter where "a control computer program (or a software-management computer program)" as recited in the claim does not fall into any category of statutory classes defined in 35 U.S.C 101 because (a) the claim is merely directed to a functional descriptive material (i.e. software, per se), and is not technologically embodied in a tangible medium, and (b) the claim may be reasonably interpreted as a digital signal (SPEC: Page130 Line 21 – 22: e.g., a computer program realized by a digital signal) and therefore the claim is directed to a non-statutory subject matter as not being tangible and concrete. It is suggested by the Examiner to incorporate the limitations by being embodied on a computer readable recording /

storage medium (e.g. its dependent respective claims 20 and 23). By not limiting the computer program to being stored on a computer readable recording / storage medium, there is a lack of the required functional and structural interrelationship between the software and the computer recording / storage medium that permits the functionality of the software to be realized upon access by a processor. This ability is what underlies the ability to provide a practical application. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106 (IV.B).1(a).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 5, 6, 11 and 18 – 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Otsuka et al. (U.S. Patent 6,094,723).

As per claim 5, Otsuka teaches a recording medium (Otsuka: Figure 1D), comprising:

a normal storage unit having stored therein software that is computer data (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67 and Column 10 Line 14 – 21: the CD ARW (a rewritable area) that stores file system software and install management file/data such as the number of times the installation has been performed is considered as a normal storage unit);

a secure storage unit not directly accessible from outside, and having stored therein license information relating to a usage condition of the software (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45 and Column 10 Line 14 – 21: the CD AE (a read-only ROM area) that stores "install system" including an install system software module and the number of N_p permitted installations that <u>prevents</u> user illegal changes from outside and <u>increases</u> the security management is qualified as a secure storage unit); and

a tamper-resistant module (Otsuka: Figure 14 / Element 90: "<u>Install System</u>" that is stored in the CD AE (a read-only ROM area) is qualified as a tamper-resistant module) **operable to judge, based on the license information, whether an operation, being one of installing software on an information-processing device and deactivating installed software, is permitted** (Otsuka: Figure 16 / Element F103 – F108, Column 1 Line 51 – 59 / Line 60 – 65, Column 16 Line 36 – 62 / Line 43 – 46, Column 13 Line 1 – 5 and Column 20 Line 1 – 8: an "Install System" software module stored at the CD read-only AE area is employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security), **and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted** (Otsuka: Column 13 Line 15 –

15 and Column 18 Line 66 – 67: the host system operates, based on the "Install System", is taking the instruction of permission from the "Install System" to proceed installation / un-installation application programs), **and to rewrite the license information in accordance with the operation** (Otsuka: Column 20 Line 5 – 7: directly updates the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security).

As per claim 18, Otsuka teaches a control method used by a recording medium that includes a normal storage unit having stored therein software that is computer data (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67 and Column 10 Line 14 – 21: the CD ARW (a rewritable area) that stores file system software and install management file/data such as the number of times the installation has been performed is considered as a normal storage unit), a secure storage unit not directly accessible from outside and having stored therein license information relating to a usage condition of the software (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45 and Column 10 Line 14 – 21: the CD AE (a read-only ROM area) that stores "install system" including an install system software module and the number of N_p permitted installations that <u>prevents</u> user illegal changes from outside and <u>increases</u> the security management is qualified as a secure storage unit), and a tamper-resistant module (Otsuka: Figure 14 / Element 90: "<u>Install System</u>" that is stored in the CD AE area is qualified as a tamper-resistant module), comprising the steps of:

judging, based on the license information, whether an operation, being one of installing software on an information-processing device and deactivating installed software, is permitted (Otsuka: Figure 16 / Element F103 – F108, Column 1 Line 51 – 59 / Line 60 – 65, Column 16 Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8: an "Install System" software module stored at the CD read-only AE area is employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security);

outputting to the information-processing device when judged in the affirmative, an instruction showing the operation to be permitted (Otsuka: Column 13 Line 15 – 15 and Column 18 Line 66 – 67: the host system operates, based on the "Install System", is taking the instruction of permission from the "Install System" to proceed installation / un-installation application programs); and

rewriting the license information in accordance with the operation (Otsuka: Column 20 Line 5 – 7: directly updates the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security).

As per claim 19, Otsuka teaches a control computer program used by a recording medium that includes a normal storage unit having stored therein software that is computer data (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67 and Column 10

Line 14 – 21: the CD ARW (a rewritable area) that stores file system software and install management file/data such as the number of times the installation has been performed is considered as a normal storage unit), a secure storage unit not directly accessible from outside and having stored therein license information relating to a usage condition of the software (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45 and Column 10 Line 14 – 21:.the CD AE (a read-only ROM area) that stores "install system" including an install system software module and the number of N_p permitted installations that prevents user illegal changes from outside and increases the security management is qualified as a secure storage unit), and a tamper-resistant module (Otsuka: Figure 14 / Element 90: "Install System" that is stored in the CD AE area is qualified as a tamper-resistant module), comprising the steps of:

judging, based on the license information stored in the secure storage unit, whether an operation, being one of installing software on an information processing device and deactivating installed software, is permitted (Otsuka: Figure 16 / Element F103 – F108, Column 1 Line 51 – 59 / Line 60 – 65, Column 16 Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8: an "Install System" software module stored at the CD read-only AE area is employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security);

outputting to the information-processing device when judged in the affirmative,. an instruction showing the operation to be permitted (Otsuka: Column 13 Line 15 – 15 and

Column 18 Line 66 – 67: the host system operates, based on the "Install System", is taking the instruction of permission from the "Install System" to proceed installation / un-installation application programs); and

rewriting the license information in accordance with the operation (Otsuka: Column 20 Line 5 – 7: directly updates the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security).

As per claim 6, Otsuka teaches **the normal storage unit stores the software, being one of a computer program and digital data** (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67 and Column 10 Line 14 – 21: the CD ARW (a rewritable area) that stores file system software and install management file/data such as the number of times the installation has been performed is considered as a normal storage unit), **the secure storage unit stores the license information, which relates to a usage condition of one of the computer program and the digital** data (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45 and Column 10 Line 14 – 21: the CD AE (a read-only ROM area) that stores "install system" including an install system software module and the number of N_p permitted installations that <u>prevents</u> user illegal changes from outside and <u>increases</u> the security management is qualified as a secure storage unit), **and the tamper-resistant module** (Otsuka: Figure 14 / Element 90: "<u>Install System</u>" that is stored in the CD AE area is qualified as a tamper-resistant module) **judges whether the operation, being one of (i) installing or uninstalling the computer program**

with respect to the information-processing device and (ii) duplicating or deleting the digital data, is permitted (Otsuka: Figure 16 / Element F103 – F108, Column 1 Line 51 – 59 / Line 60 – 65, Column 16 Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8: an "Install System" software module stored at the CD read-only AE area is employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security: installing or uninstalling the computer program).

As per claim 11, Otsuka teaches **the secure storage unit stores a part rather than a whole of the license information** (Otsuka: Column 12 Line 42 – 45: the CD AE (a read-only ROM area) that stores the number of N_p permitted installations that prevents user illegal changes from outside and increases the security management is qualified as a secure storage unit), **and the tamper-resistant module stores the remaining part of the license information, extracts the part of the license information stored in the secure storage unit, generates the license information from the extracted part and the stored remaining part, and performs the judgment based on the generated license information** (Otsuka: Column 16 Line 66 – Column 17 Line 3: the decryption / encryption functions, that are stored at the Install System (i.e. the tamper-resistant module) to enable the system to update the install management file are considered as part of the license information).

As per claim 20, Otsuka teaches the computer program being stored on a computer-readable recording medium (Otsuka: Figure 11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 12 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuka et al. (U.S. Patent 6,094,723).

As per claim 12, Otsuka teaches **the license information is a permitted usage count of the software** (Otsuka: Column 12 Line 42 – 45: the CD AE (a read-only ROM area) that stores the number of N_p permitted installations that <u>prevents</u> user illegal changes from outside and <u>increases</u> the security management), **and the tamper-resistant module judges whether installation is permitted by judging whether the permitted usage count is greater than 0, judges that installation of the software is permitted when judged to be greater than 0, outputs the instruction, and writes the permitted usage count to the secure storage unit after reducing the count by 1** (Otsuka: Column 1 Line 50 – 59 and Column 13 Line 1 – 9: <u>Examiner notes</u> Otsuka teaches using two separate parameters, namely N_p and Ni, where N_p stores the fixed total number of times the software are permitted to be installed and Ni stores the number of times that the software has been installed and therefore it is considered as obviously equivalent to reducing the permitted usage count N_p by 1 after each software installation).

As per claim 13, Otsuka teaches **the license information is a permitted usage count of the software** (Otsuka: Column 12 Line 42 – 45: the CD AE (a read-only ROM area) that stores the number of N_p permitted installations that prevents user illegal changes from outside and increases the security management), **and the tamper-resistant module outputs the instruction when judged that deactivation of the software is permitted, and writes the permitted usage count to the secure storage unit after increasing the count by 1** (Otsuka: Column 1 Line 60 – 65 and Column 23 Line 20 – 26: Examiner notes Otsuka teaches using two separate parameters, namely N_p and Ni, where (a) decreasing the Ni by one (i.e. decreasing the number of times that the software has been installed) (b) N_p stores the fixed total number of times the software are permitted to be installed and therefore it is considered as obviously equivalent to increasing the permitted usage count N_p by 1 after each software de-installation).

8. Claims 1 – 4, 15 and 20 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuka et al. (U.S. Patent 6,094,723), in view of Tagawa et al. (U.S. Patent 7,096,504).

As per claim 1, Otsuka teaches **a software-management system comprising a recording medium and an information-processing device** (Otsuka: Figure 1 and 11), the recording medium (Otsuka: Figure 1D) including:

a normal storage unit having stored therein software that is computer data (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67 and Column 10 Line 14 – 21: the CD ARW (a rewritable area) that stores file system software and install management file/data such as the number of times the installation has been performed is considered as a normal storage unit) and;

a secure storage unit not directly accessible from outside, and having stored therein license information relating to a usage condition of the software (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45 and Column 10 Line 14 – 21: the CD AE (a read-only ROM area) that stores "install system" including an install system software module and the number of N_p permitted installations that <u>prevents</u> user illegal changes from outside and <u>increases</u> the security management is qualified as a secure storage unit); and

a tamper-resistant module (Otsuka: Figure 14 / Element 90: "<u>Install System</u>" that is stored in the CD AE area is qualified as a tamper-resistant module) **operable to judge, based on the license information, whether an operation, being <u>one of</u> installing software on the information-processing device and deactivating installed software, is permitted** (Otsuka: Figure 16 / Element F103 – F108, Column 1 Line 51 – 59 / Line 60 – 65, Column 16 Line 36 – 62 / Line 43 – 46, Column 13 Line 1 – 5 and Column 20 Line 1 – 8: an "Install System" software module stored at the CD read-only AE area is employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security), **and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted** (Otsuka: Column 13 Line 15 – 15 and Column 18 Line 66 – 67: the host system operates, based on the "Install System", is taking the instruction of permission from the "Install System" to proceed installation / un-installation application programs), **and to rewrite the license information in accordance with the operation** (Otsuka: Column 20 Line 5 – 7: directly updates the install management file such as the number Ni (# times been installed) w/o going through the user file system to increase the security), and

the information-processing device (Otsuka: Figure 11 / Element 1 & 2: the integral part of a recording / reproduction apparatus and associated host computer interface is considered as an information-processing device: i.e. the recording medium is attached to an information-processing device that is also consistent with the instant specification (SPEC: Figure 1 / Element 200 & 300) including:

a control unit operable to perform, in accordance with the received instruction, one of (i) receiving software from the recording medium and installing the received software in the information-processing device, and (ii) deactivating installed software (Otsuka: Figure 11 / Element 1 & 2 and Column 9 Line 8 – 15);

However, Otsuka does not teach a receiving unit operable to receive the instruction from the recording medium.

Tagawa teaches **a receiving unit operable to receive the instruction from the recording medium** (Tagawa: FIG. 3C & 4D / 4C, Column 2 Line 3 – 7, Column 9 Line 42 – 48 and Column 7 Line 42 – 46: the connected compatible device is considered as the receiving unit and the memory card, including the security processing units, is considered as the removable recording medium (e.g., consistent with the disclosure in the instant specification (SPEC: Figure 3 / Element 211 and 213) that can communicate to an receiving unit because (a) Tagawa teaches "a compatible device is connected to the memory card, whose protected area stores a Usage Rule and if the Usage Rule indicates that the number of permitted times is "0", the connected device cannot obtain management rights (i.e. usage information / rule) from the memory card (Tagawa: FIG. 3C & 4D / 4C and Column 9 Line 42 – 48) and (b) Examiner notes if the connected device cannot obtain usage information / rule from the memory card, then the connected device (i.e. the information processing device) has no way to make any determination by itself whether the permission should be granted or not and as such the permission instruction is obviously equivalent to be determined solely from the authentication / encryption processing unit on the memory card accordingly).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Tagawa within the system of Otsuka because (a) Otsuka teaches a recording medium contains a plurality of storage units (incl. protected area) that stores license / usage information / rule and a tamper-resistant module; however, the license information and tamper-resistant module (i.e. Install System) need to be read-out by the connected host system (due to the lack of processing unit in the recording medium) in order to be executed to determine whether the access control permission should be granted (Otsuka: Figure 1D & 19, Column 10 Line 5 – 8, Column 12 Line 39 – 45 and Column 10 Line 14 – 21, Figure 16 / Element F103 – F108, Column 16 Line 36 – 62 / Line 43 – 46 , Column 13 Line 1 – 5 and Column 20 Line 1 – 8), and (b) Tagawa teaches providing a distribution system that provides a high level of convenience for the user, while protecting copyright with an security enhanced structure by using a memory card (i.e. a removable recording medium) that contains not only a plurality of storage units (incl. protected area) storing usage information / rule but also includes security processing units (i.e. authentication and encryption units) so that the secured data can be better isolated and protected on the memory card accordingly (Tagawa: FIG. 3C & 4D / 4C, Column 2 Line 3 – 7, Column 9 Line 42 – 48 and Column 7 Line 42 – 46 & also see the same rationale as set forth above).

As per claim 15, the claim limitations encompasses the same scope as described in claim 1 and the only difference is the reverse of the claim <u>reciting sequence</u> in the group of limitations regarding the information-processing device (1st – 2nd claim limitations) and the recording medium (4th – 6th claim limitations). See the same rationale set forth as above in rejecting claim 1.

As per claim 21 and 22, the claim limitations encompass the same scope as described in claim 15. See the same rationale set forth as above in rejecting claim 15.

As per claim 2, Otsuka as modified teaches a software-writing device (Otsuka: Figure 11 / Element 2 & 3: the integral part of a hard disk driver and associated host computer interface is considered as a software-writing device) that includes:

an information-storage unit having stored therein software that is computer data, and license information relating to a usage condition of the software (Otsuka: Otsuka: Figure 11 / Element 2 & 3 and Column 8 Line 58 – 67 and Column 9 Line 56 – 58);

a reading unit operable to read the software and the license information from the information-storage unit (Otsuka: Figure 11 / Element 2 & 3 and Column 8 Line 58 – 67 and Column 9 Line 56 – 58); and

an output unit operable to output the read software and license information (Otsuka: Otsuka: Figure 11 / Element 2 & 3 and Column 8 Line 58 – 67 and Column 9 Line 56 – 58),

wherein the recording medium further includes:

a receiving unit operable to receive the software and the license information (Otsuka: Figure 11 / Element 11/ 12 / 13 / 19 and Column 7 Line 40 – 49: the removable recording medium using the recording and reproduction apparatus to support the RD/WR functions to the recording medium); and

a writing unit operable to write the received software to the normal storage unit and the received license information to the secure storage unit (Otsuka: Figure 11 /

Element 11/ 12 / 13 / 19 and Column 7 Line 40 – 49: the removable recording medium using the recording and reproduction apparatus to support the RD/WR functions to the recording medium).

As per claim 3, Otsuka as modified teaches the software-writing and information-processing devices are connected to each another via a network (Otsuka: Figure 11 / Element 1 / 3 / 2 and Column 19 Line 37: a recording and reproduction apparatus and a hard disk driver can be connected in a network through a host system which is also used as a server), the output unit of the software-writing device outputs the software securely via the network (Otsuka: Column 17 Line 8 – 12: the software can be securely encrypted), the information-processing device further includes: a receiving unit operable to receive the software securely via the network; and an output unit operable to output the received software to the recording medium (Otsuka: Figure 11 / Element 3 / 2 / 1: receiving software from the host system / server over the network and output the received software to the controller, Figure 11 / Element 11, of the recording medium), and the receiving unit of the recording medium receives the software from the information-processing device (Otsuka: Figure 11 / Element 11 / 1: the controller is considered as part of the integral receiving unit of the recording medium).

As per claim 4, Otsuka as modified teaches a distribution device (Otsuka: Figure 11 / Element 2 and Column 19 Line 37: a host system which is also used as a server connected within a network can be considered as a distribution device), wherein the software-writing, information-processing, and distribution devices are connected to each another via a network (Otsuka: Figure 11 / Element 2 / 3 / 1 and Column 19 Line 37: see the same rationale set forth as above in claim 3), the output unit of the software-writing device outputs the license information securely via the network (Otsuka: Column 20 Line 6 – 8: the install management file can be encrypted), the information-processing device further includes: a receiving unit operable to receive the license information securely via the network; and an output unit operable to output the received license information to the recording medium (Otsuka: Figure 11 / Element 3 / 2 / 1: receiving software from the host system / server over the network and output the received software to the controller, Figure 11 / Element 11, of the recording medium as part of the recording and reproduction apparatus), and the receiving unit of the recording medium receives the license information from the information-processing device (Otsuka: Figure 11 / Element 11 / 12 / 13).

As per claim 23, Otsuka as modified teaches the computer program being stored on a computer-readable recording medium (Otsuka: Figure 11).

9. Claims 7 – 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuka et al. (U.S. Patent 6,094,723), in view of Talstra et al. (U.S. Patent 2005/0076225).

As per claim 7, Otsuka teaches the normal storage unit stores the software, being one of a computer program and digital data (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67 and Column 10 Line 14 – 21) that have been encrypted using a soft key Column 17 Line 8 – 12: the software can be securely encrypted), the secure storage unit stores the license information (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45 and Column 10 Line 14 – 21: the CD AE (a read-only ROM area) that stores "install system" including an install system software module and the number of Np permitted installations that <u>prevents</u> user illegal changes from outside and <u>increases</u> the security management is qualified as a secure storage unit).

However, Otsuka does not disclose expressly the secure storage unit stores the soft key.

Talstra teaches the secure storage unit stores the soft key (Talstra: Para [0037] Line 6 – 10 and Figure 2: an Effective Key Block (EKB) is stored in a <u>read-only</u> channel by using a wobble techniques in a record / playback medium).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Talstra within the system of Otsuka because (a) Otsuka teaches providing a recording medium system / apparatus that contains a plurality of storage units (incl. protected area) that stores license / usage information / rule and a tamper-resistant module and the software/ data can be securely encrypted (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45, Column 10 Line 14 – 21 and Column 17 Line 8 – 12) and (b) Talstra teaches, in a recording / playback system, the digital right information such as the encryption key block and the associated digital signature can be securely stored in a read-only channel on the disk (Talstra: Para [0037], [0006] and [0040]).

Otsuka in view of Talstra teaches:

the tamper-resistant module (Otsuka: Figure 14 / Element 90: "Install System" that is stored in the CD AE area is qualified as a tamper-resistant module), when installation is judged to be permitted, extracts the soft key from the license information, and outputs the instruction with the extracted soft key included therein (Otsuka: Figure 16 / Element F103 – F108, Column 16 Line 64 – 67 / Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8 & Talstra: Para [0037] Line 6 – 10: (a) the Install System has decryption function and is also employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) and as such (b) the soft key must be extracted for decryption purpose).

As per claim 8, Otsuka teaches the secure storage unit stores the license information (Otsuka: Figure 11 / Element 11/ 12 / 13 / 19 and Column 7 Line 40 – 49).

However, Otsuka does not disclose expressly including signature data relating to the software.

Talstra teaches including signature data relating to the software (Talstra: Para [0006] Last sentence and Figure 2: a cryptographic hash / signature over an Effective Key Block (EKB) that is related to the software is also stored in a read-only channel by using a wobble techniques in a record / playback medium). See same rationale of combination applied herein as above in rejecting the claim 7.

Otsuka in view of Talstra teaches:

the tamper-resistant module (Otsuka: Figure 14 / Element 90: "Install System" that is stored in the CD AE area is qualified as a tamper-resistant module), when installation is judged to be permitted, extracts the signature data from the license information, and outputs the instruction with the extracted signature data included therein (Otsuka: Figure 16 / Element F103 – F108, Column 16 Line 64 – 67 / Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8 & Talstra: Para [0037] Line 6 – 10 and Para [0006] Last sentence: (a) the Install System has decryption function and is also employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) and as such (b) the soft key must be extracted and validated by the corresponding digital signature for decryption purpose).

As per claim 9, the claim limitations are met as the same reasons as that set forth in the paragraph above regarding to claim 8 with the exception of the feature extracting the signature data from the license information, and outputs the extracted signature data instead of the instruction (Otsuka: Figure 16 / Element F103 – F108, Column 16 Line 64 – 67 / Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8 & Talstra: Para [0037] Line 6 – 10 and Para [0006] Last sentence: Examiner notes it would have been obvious to a person of ordinary skill in the art at the time the invention to recognize outputting the extracted signature data prior to outputting the instruction (as an option) because the license information / usage software need to be decrypted by the correct decryption / encryption key block first which is validated by the EKB signature information and then the instruction whether the permission should be granted or not based on the decrypted usage information can be subsequently determined – Also refer to the Claim Objection section set forth above).

As per claim 10, Otsuka teaches the secure storage unit stores the license information, which is generated by encrypting the usage condition using predetermined key information (Otsuka: Figure 1D & 19, Column 12 Line 65 – 67, Column 10 Line 14 – 21 and Column 17 Line 8 – 12: the software can be securely encrypted).

However, Otsuka does not disclose expressly the tamper-resistant module stores the key information.

Talstra teaches the tamper-resistant module stores the key information (Talstra: Para [0037] Line 6 – 10 and Figure 2: an Effective Key Block (EKB), i.e. digital right, is stored in a read-only channel by using a wobble techniques in a record / playback medium).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Talstra within the system of Otsuka because (a) Otsuka teaches providing a recording medium system / apparatus that contains a plurality of storage units (incl. protected area – i.e. secure storage unit) that stores license / usage information / rule and a tamper-resistant module and the software/ data can be securely encrypted (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45, Column 10 Line 14 – 21 and Column 17 Line 8 – 12) and (b) Talstra teaches, in a recording / playback system, the digital right information such as the encryption key block can be securely stored in a read-only channel on the disk (Talstra: Para [0037] and [0040]: a secure storage unit that stores the tamper-resistant module / usage information).

Otsuka in view of Talstra teaches:

the tamper-resistant module stores the key information, decrypts the license information using the key information to generate the usage condition, and performs the judgment based on the generated usage condition (see the same rationale as set forth above in claim 7 – 9).

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuka et al. (U.S. Patent 6,094,723), in view of Jones et al. (U.S. Patent 2002/0111996).

As per claim 14, Otsuka teaches the install control program references verification information as part of the license information to determine the installation or un-installation is allowed or not and the verification information is time information (Otsuka: Column 24 Line 9 – 10 and Column 23 Line 65 – Column 24 Line 7).

However, Otsuka does not disclose expressly the license information is a permitted usage period of the software.

Jones teaches the license information is a permitted usage period of the software (Jones: Para [0295]: maximum permitted period of time in included in the license information).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Jones within the system of Otsuka because (a) Otsuka teaches providing a verification information as a time information to determine the installation or un-installation of software is allowed or not as part of the license information (Otsuka: Column 24 Line 9 – 10 and Column 23 Line 65 – Column 24 Line 7) and (b) Jones teaches the license information can a permitted usage period of the software (Jones: Para [0295] and [0289]: maximum permitted period of time in included in the license information).

Otsuka in view of Talstra teaches:

the tamper-resistant module judges whether installation is permitted by judging whether a current date-time is within the permitted usage period, judges that installation of the software is permitted when judged to be within the permitted usage period, and outputs the instruction (Otsuka: Column 24 Line 9 – 10 and Column 23 Line 65 – Column 24 Line 7, Figure 16 / Element F103 – F108, Column 16 Line 64 – 67 / Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8, Column 13 Line 15 – 15 and Column 18 Line 66 – 67 & Jones: Para [0295] and [0289]: the Install System manages the installation / un-installation application programs by using time verification information and the host system operates, based on the "Install

System", is taking the instruction of permission from the "Install System" to proceed installation / un-installation application programs).

11. Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuka et al. (U.S. Patent 6,094,723), in view of Tagawa et al. (U.S. Patent 7,096,504), and in view of Talstra et al. (U.S. Patent 2005/0076225).

As per claim 16, Otsuka as modified teaches the secure storage unit of the recording medium stores the license information (Otsuka: Figure 11 / Element 11/ 12 / 13 / 19 and Column 7 Line 40 – 49), Otsuka does not disclose expressly including signature data relating to the software.

Talstra teaches including signature data relating to the software (Talstra: Para [0006] Last sentence and Figure 2: a cryptographic hash / signature over an Effective Key Block (EKB) that is related to the software is also stored in a read-only channel by using a wobble techniques in a record / playback medium).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Talstra within the system of Otsuka as modified because (a) Otsuka teaches providing a recording medium system / apparatus that contains a plurality of storage units (incl. protected area) that stores license / usage information / rule and a tamper-resistant module and the software/ data can be securely encrypted (Otsuka: Figure 1D & 19, Column 12 Line 39 – 45, Column 10 Line 14 – 21 and Column 17 Line 8 – 12) and (b) Talstra teaches, in a recording / playback system, the digital right information such as the encryption key block and the associated digital signature can be securely stored in a read-only channel on the disk (Talstra: Para [0037], [0006] and [0040]).

Otsuka as modified teaches:

the tamper-resistant module (Otsuka: Figure 14 / Element 90: "Install System" that is stored in the CD AE area is qualified as a tamper-resistant module) of the recording medium, when installation is judged to be permitted, extracts the signature data from the license information, and outputs the instruction with the extracted signature data included therein (Otsuka: Figure 16 / Element F103 – F108, Column 16 Line 64 – 67 / Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8 & Talstra: Para [0037] Line 6 – 10 and Para [0006] Last sentence: (a) the Install System has decryption function and is also employed by the host system to manage the installation / un-installation application programs that can directly control the device driver and to update the install management file such as the number Ni (# times been installed) and as such (b) the ciphering key must be extracted and validated by the corresponding digital signature for decryption purpose), the receiving unit receives the instruction with the signature data included therein, and the control unit performs one of (i) verifying a correctness of software received from the recording medium using the received software and the signature data included in the received instruction (Talstra : Para [0007]: one piece of the signature is considered as the signature of the EKB key block data to assure the ciphering keys are correct) and (ii) verifying a correctness of software installed in the information-processing device using the installed software and the signature data included in the received instruction, and if verification is successful, performs the operation (Talstra : Para [0018]: another piece of the signature is considered as the signature data generated from the associated application software received from the recording medium because Talstra teaches validating the system data integrity with the received signature data and the system data can be **any kind** of data integrity of which shall be checked and thus it would have been obvious to a person of ordinary skill in the art at the time the invention to recognize the checking may include the received software integrity check).

As per claim 17, the claim limitations are met as the same reasons as that set forth in the paragraph above regarding to claim 16 with the exception of the feature extracting the signature data from the license information, and outputs the extracted signature data instead of the instruction (Otsuka: Figure 16 / Element F103 – F108, Column 16 Line 64 – 67 / Line 36 – 62, Column 13 Line 1 – 5, Column 16 Line 43 – 46 and Column 20 Line 1 – 8 & Talstra: Para [0037] Line 6 – 10 and Para [0006] Last sentence: Examiner notesvit would have been obvious to a person of ordinary skill in the art at the time the invention to recognize outputting the extracted signature data prior to outputting the instruction (as an option) because the license information / usage software need to be decrypted by the correct decryption / encryption key block first which is validated by the EKB signature information and then the instruction whether the permission should be granted or not based on the decrypted usage information can be subsequently determined – Also refer to the Claim Objection section set forth above).

Otsuka as modified teaches:

the receiving unit receives the signature data (Talstra : Para [0018] and [0015] & Otsuka: Figure 11 / Element 1 & 2), and the control unit verifies a correctness of software received from the recording medium using the received the signature data, and if verification is successful, installs the received software in the information-processing device (Talstra : Para [0018]: Talstra teaches validating the system data integrity with the received signature data and the system data can be **any kind** of data integrity of which shall be checked and thus it would have been obvious to a person of ordinary skill in the art at the time the invention to recognize the checking may include the received software integrity check).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai

Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
4/15/2007